BASIC PROFESSIONAL TRAINING COURSE

Module XI

Operational Limits and Conditions
Background

In 1991, the General Conference (GC) in its resolution RES/552 requested the Director General to prepare ‘a comprehensive proposal for education and training in both radiation protection and in nuclear safety’ for consideration by the following GC in 1992. In 1992, the proposal was made by the Secretariat and after considering this proposal the General Conference requested the Director General to prepare a report on a possible programme of activities on education and training in radiological protection and nuclear safety in its resolution RES1584.

In response to this request and as a first step, the Secretariat prepared a Standard Syllabus for the Postgraduate Educational Course in Radiation Protection. Subsequently, planning of specialised training courses and workshops in different areas of Standard Syllabus were also made. A similar approach was taken to develop basic professional training in nuclear safety. In January 1997, Programme Performance Assessment System (PPAS) recommended the preparation of a standard syllabus for nuclear safety based on Agency Safety Standard Series Documents and any other internationally accepted practices. A draft Standard Syllabus for Basic Professional Training Course in Nuclear Safety (BPTC) was prepared by a group of consultants in November 1997 and the syllabus was finalised in July 1998 in the second consultants meeting.

The Basic Professional Training Course on Nuclear Safety was offered for the first time at the end of 1999, in English, in Saclay, France, in cooperation with Institut National des Sciences et Techniques Nucléaires/Commissariat a l'Energie Atomique (INSTN/CEA). In 2000, the course was offered in Spanish, in Brazil to Latin American countries and, in English, as a national training course in Romania, with six and four weeks duration, respectively. In 2001, the course was offered at Argonne National Laboratory in the USA for participants from Asian countries. In 2001 and 2002, the course was offered in Saclay, France for participants from Europe. Since then the BPTC has been used all over the world and part of it has been translated into various languages. In particular, it is held on a regular basis in Korea for the Asian region and in Argentina for the Latin American region.

In 2015 the Basic Professional Training Course was updated to the current IAEA nuclear safety standards. The update includes a BPTC text book, BPTC e-book and 2 “train the trainers” packages, one package for a three month course and one package is for a one month course. The” train the trainers” packages include transparencies, questions and case studies to complement the BPTC.

This material was prepared by the IAEA and co-funded by the European Union.

Editorial Note

The update and the review of the BPTC was completed with the collaboration of the ICJT Nuclear Training Centre, Jožef Stefan Institute, Slovenia and IAEA technical experts.
# Contents

1 CONCEPT OF OPERATIONAL LIMITS AND CONDITIONS ................................................................. 5

1.1 Basic concepts .............................................................. 5
   Objectives and bases of OLCs ........................................ 5
   Scope of OLCs ................................................................ 6
   Implementation of OLCs ............................................... 7

1.2 Questions ...................................................................... 7

2 SAFETY LIMITS ..................................................................... 8

2.1 The First Safety Limit .................................................... 8

2.2 The Second Safety Limit ............................................... 9

2.3 Questions ...................................................................... 9

3 SAFETY SYSTEM ................................................................ 10

3.1 Introduction .................................................................. 10

3.2 Defence-in-Depth ........................................................ 11

3.3 General principles used for designing the safety system13
   Integrity of the fuel cladding ........................................... 13
   Integrity of the reactor coolant system ............................. 14
   Integrity of the Containment ........................................... 14

3.4 Reactor protection system .......................................... 14
   List of reactor trips ....................................................... 16

3.5 Questions .................................................................... 20

4 LIMITS AND CONDITIONS FOR NORMAL OPERATION22

4.1 General considerations ............................................... 22

4.2 Reactivity control ......................................................... 23
   Negative reactivity requirements ................................. 23
   Reactivity coefficients ................................................ 23
   Positive reactivity insertion rates ................................... 23
   Reactor core neutron flux monitoring ............................ 23
   Reactivity control logic ................................................ 23
   Reactivity control devices .......................................... 24
   Reactivity differences ............................................... 24
   Liquid poison systems ................................................. 24
   Boron dilution prevention .......................................... 24
   Reactor protection system .......................................... 24

4.3 Core cooling ................................................................ 24
   Coolant temperature .................................................. 24
   Coolant pressure ....................................................... 25
   Reactor power and power distribution .......................... 25
   Safety and relief valves ............................................ 25
   Steam generators ...................................................... 25
   Coolant system leakage ........................................... 25
   Radioactivity in the coolant ....................................... 25
   Ultimate heat sink ..................................................... 26
   Decay heat removal ................................................... 26
   Emergency core cooling .......................................... 26

4.4 Coolant and moderator chemistry ............................... 26
   Reactor coolant chemical quality ............................... 26
   Moderator and cover gas system ............................... 26
Module XI: Operational Limits and Conditions

Failed fuel detection .......................................................... 26

4.5 Containment systems and accident management systems ............................................................................. 26

4.6 Electrical power systems ................................................... 27

4.7 Other systems .................................................................. 27

Ventilation systems ............................................................. 27

Seismic monitors ................................................................. 27

Fuel handling ...................................................................... 28

Irradiated fuel storage ......................................................... 28

New fuel storage ................................................................. 28

Core verification ................................................................. 28

Radiation monitoring .......................................................... 28

External events .................................................................... 29

4.8 Questions ....................................................................... 29

5 OPERATIONAL LIMITS AND CONDITIONS DOCUMENT – TECHNICAL SPECIFICATIONS ............................................................................. 30

5.1 Introduction ..................................................................... 30

5.2 An example of TS (Westinghouse PWR) ......................... 31

  Definitions ......................................................................... 31

Safety Limits and Limiting Safety System Settings ................. 32

Limiting Conditions for Operation (LCO) ............................ 32

Design features ................................................................. 34

Administrative controls ..................................................... 34

Basis .................................................................................. 34

5.3 Questions ....................................................................... 34

6 CASE STUDY ........................................................................ 35

  Range of steady state operation ........................................ 35

  Alarm setting exceeded (curve No. 1) .............................. 35

  Operational limit exceeded (curve No. 2) ......................... 35

  Safety system setting exceeded (curve No. 3) .................. 36

  Safety limit exceeded (curve No. 4) ................................. 37

6.1 Questions ....................................................................... 37

7 REFERENCES ....................................................................... 38
1 CONCEPT OF OPERATIONAL LIMITS AND CONDITIONS

Learning objectives
After completing this chapter, the trainee will be able to:
1. Explain the bases and objectives of operational limits and conditions (OLCs).
2. List items included in OLCs.
3. Explain the implementation of OLCs.

For a nuclear power plant to be operated in a safe manner, the provisions made in the final design and subsequent modifications are reflected in the limitations on plant operating parameters, and in the requirements on plant equipment and personnel. Under the responsibility of the operating organization, these are developed during the design safety evaluation as a set of operational limits and conditions (OLCs). A major contribution to compliance with the OLCs is made by the development and utilization of operating procedures that are consistent with and fully implement the OLCs.

Operational limits and conditions are at the junction between design and safety analysis and plant operations. The OLCs are that part of the operating rules, derived from the design and safety analysis report, that assure that the plant is operated in accordance with its design basis, as well as in accordance with its licence conditions.

The technical aspects of the OLCs cover the limitations that are observed, as well as the operational requirements that structures, systems and components important to the safety of the nuclear power plant meet in order to perform their intended functions as assumed in the plant safety analysis report. Safe operation depends upon personnel as well as on equipment; OLCs therefore also cover the actions that are taken and the limitations that are observed by operating personnel.

1.1 Basic concepts

Objectives and bases of OLCs
The basic objectives of OLCs are to prevent operational situations that might lead to accident conditions, and to assure that mitigation is available if an accident should occur. The OLCs restrict operation of the plant in such a manner that all plant parameters are within the design basis. Thus, if a postulated initiating event were to occur, the control and safety systems will function as designed to prevent excessive radioactive release. The OLCs are based on the whole safety assessment of the plant, both deterministic and probabilistic, including not only the analysis of plant performance, but also issues such as surveillance and testing requirements for safety systems, allowable
system outage times, etc. In recent years, the use of probabilistic safety assessment (PSA) insights in evaluating surveillance, testing, and maintenance requirements for plant systems has increased significantly. This so-called “risk-based maintenance” is one of the most practical applications of PSA in plant operations.

**Scope of OLCs**

Operational limits and conditions consider all aspects of plant operation that bear on safety, including not only the process related aspects such as power level, pressure, temperature, flow, and the like, but also equipment status, personnel status, the existence of potential external threats, etc. The OLCs at the power plant include the following items:

- **Safety limits**: limits to process variables within which the plant operation is safe;
- **Safety system settings**:
  - Limits at which the Reactor Protection System (RPS) activates reactor trip to prevent Safety Limits being exceeded;
  - Limits at which the RPS activates the Engineering Safety Features Actuation System (ESFAS) that starts the Engineering Safety Features (ESF) systems to mitigate core damage during an accident condition.
- **Limits and conditions for normal operation**: these include limits on normal process variables, as well as requirements for minimum staffing, minimum operable equipment, and allowable outage times for systems and equipment;
- **Surveillance requirements**: requirements for periodic checks, tests, calibrations, and inspections of equipment, components, and processes to establish operability, performance, correct set points, and to assure reliability; and
- **Action statements**: statements of actions to be taken by operating staff in the event of various abnormal conditions, which may take the form of emergency operating instructions or similar procedures.

In addition, OLCs may include objectives for all or some of the most significant OLCs in order to justify their application, as well as forming a basis for their derivation. These items are included in the documentation on OLCs to increase consciousness on the part of plant personnel of their application and observance.

The OLCs include requirements related to all modes of normal operation, including:

- Approach to reactor criticality;
- Start-up and power ascension;
- Operation at steady power;
- Manoeuvring - power increase and decrease;
- Shutdown to hot standby;
- Shutdown to cold standby;
- Operations conducted with the reactor shutdown, such as fuel handling;
- Maintenance, surveillance, and testing both during operation and shutdown.

**Implementation of OLCs**

Operational limits and conditions are implemented in the Technical Specifications (TS) document for the plant, and reflected in operating instructions and procedures. It is essential that the OLCs are readily available to operators, technical support personnel, and maintenance personnel. It is particularly important that the information and limits are stated in terms that are easily measurable and identifiable by personnel needing the information. For example, the limits on process variables of the core, heat transport systems, and energy conversion systems are stated in terms of instrument readings available in the control room. Where directly identifiable values cannot be used, the relationship of a limiting parameter with the reactor power or other measurable parameter should be indicated by tables, diagrams or computing techniques as appropriate. In modern practice, safety parameter display systems are provided in many plants to help the operators be aware of and understand the plant’s safety status.

### 1.2 Questions

1. Which operational situations are prevented by the OLCs?
2. What are the bases for the OLCs?
3. Which items are included in the OLCs?
4. List the modes of normal operation for which requirements are included in OLCs?
5. What aspects of the OLCs are important from the viewpoints of operators, technical support and maintenance personnel?
2 SAFETY LIMITS

Learning objectives
After completing this chapter, the trainee will be able to:
1. Explain the purpose of the First Safety Limit.
2. Explain the purpose of the Second Safety Limit.

2.1 The First Safety Limit

Normal operating parameters are based on the required electrical output. During transient operation it is not possible to maintain exact steady-state conditions. For transient operation worst case combinations of pressure, temperature, flow and power are analysed to set a safety limit in order to ensure fuel and cladding integrity. The limit sets constraints on the combination of average coolant temperature in the core as a function of reactor power for a given pressurizer pressure. Figure 2.1 illustrates the First Safety Limit; a $T_{avg}$ vs. power curve for a typical PWR plant at different reactor coolant system (RCS) pressures.

![Figure 2.1: First Safety Limit.](image)

Line “a” on the figure represents the maximum $T_{avg}$ (average coolant temperature) permitted at a given pressure for a particular reactor power. This curve represents prevention of the hot leg temperature $T_h$ from reaching the saturation temperature.

Line “b” is based on preventing a DNBR (Departure from the Nucleate Boiling Ratio, defined in Module 1) value less than the minimum DNBR.
Line “c” limits the coolant exiting the core to less than 15% steam.

Operation under the curve for a particular pressure ensures that:
- The min DNBR will not be less than the limiting DNBR.
- The core exit temperature is less than the saturation temperature for that pressure.

In the Technical specifications this curve is named the First Safety Limit. Reactor operation below the curve assures the integrity of the cladding of the fuel rods.

### 2.2 The Second Safety Limit

The Second Safety Limit in the Technical Specifications is a restriction on RCS pressure. The RCS pressure is limited in order to ensure the integrity of the primary system boundaries. The primary boundaries must be maintained in order to keep the radioactive coolant and the fission products released into the coolant from entering the containment or the secondary system, and potentially from the outside environment. The primary system boundaries must also be maintained because a rupture in the primary system could cause a drastic reduction in RCS pressure and consequently severe damage to the reactor core.

### 2.3 Questions

1. Which combination of parameters does the First Safety Limit represent?
2. What does operation at a certain pressure ensure?
3. What do graphs a, b, and c on the First Safety Limit diagram represent?
4. Which parameter is restricted by the Second Safety limit?
5. Why must the primary boundaries be maintained?


3 SAFETY SYSTEM

Learning objectives

After completing this chapter, the trainee will be able to:

1. Explain the purpose of the reactor safety system.
2. Describe the principle of defence-in-depth.
3. Describe the general principles used for designing the safety system.
4. Explain the purpose of the reactor protection system.
5. List reactor trip signals.

3.1 Introduction

This chapter considers the basic preliminary concepts for defining the design of the reactor safety system, namely the Reactor Protection System (RPS) and Engineering Safety Features (ESF). Reactor safety systems are designed to protect the plant in case of predetermined accident scenarios. These scenarios are grouped into categories 1 to 4 according to their decreasing probability of occurrence:

- Category 1 - Normal operation and normal operational transients.
- Category 2 - Faults of Moderate Frequency; these correspond to incidents whose occurrence frequency is estimated to be between 1 and $10^{-2}$ times per year per reactor.
- Category 3 - Infrequent faults; between $10^{-2}$ and $10^{-4}$ times per year per reactor.
- Category 4 - Limiting faults; between $10^{-4}$ and $10^{-6}$ times per year per reactor.

During category 1 events it is not necessary to trip the reactor or to start ESF systems. Expected doses due to any release are lower than the dose limits. Examples of category 1 events:

- Steady-state and shutdown operation;
- Refuelling;
- Operation with permissible deviations:
  - Fuel leak;
  - Radioactivity in Reactor Coolant System (RCS);
  - Testing allowed by TS;
  - Others.
- Operational transients:
  - Plant heat up and cool down;
  - Step load changes up to $\pm 10\%$;
  - Ramp load change up to 5%/min;
  - Load rejection;
  - Others.

During category 2 events, there is a requirement for a reactor trip, but not for the ESF systems to start. Fuel or clad damage is not expected.
The plant is immediately able to restart. Expected doses due to any release are lower than the dose limits. Examples of category 2 events:

- Feedwater water system (FWS) malfunction;
- Inadvertent opening of S/G Power Operated Relief Valve (PORV) or Safety Valve (SV);
- Inadvertent opening of Pressurizer PORV or SV;
- Inadvertent closing of Main Steam Isolation Valve (MSIV);
- Uncontrolled Rod Control Cluster Assembly (RCCA) bank withdrawal;
- Partial loss of RCS flow;
- Others.

During category 3 events, the RPS must trip the reactor and start the ESF systems. A small amount of fuel could be damaged. It is necessary to shut the plant down for a longer period of time. Expected doses due to radioactivity release are lower than dose limits. Examples of category 3 events:

- Minor Steam System piping failure;
- Complete loss of RCS flow;
- Single RCCA withdrawal at full power;
- Inadvertent loading of and operation with fuel assembly in an improper position;
- Loss of coolant accident (LOCA) from small pipes;
- Others.

Category 4 events are Design Basis Accidents (DBA). Reactor trip and start of ESF systems are needed. Fuel damage is expected. Coolable core geometry is maintained. Such an accident could lead to a definite shutdown of the power plant. Expected doses due to radioactivity release are lower than the dose limits. Examples of category 4 events:

- LOCA;
- Main Steam Line Break (MSLB);
- Feed Line Break (FLB);
- Steam Generator Tube Rupture (SGTR);
- RCCA ejection accident;
- Others.

Each category has its safety criteria that must be adhered to.

### 3.2 Defence-in-Depth

The principle of defence-in-depth is a long standing concept in the design, construction and operation of nuclear reactors, and may be thought of as requiring concentric protective barriers or means, all of which must be breached sequentially before hazardous material or dangerous energy levels can adversely affect human beings or the environment. The four classical physical barriers to radiation release are:
- Fuel;
- Cladding;
- Reactor coolant system;
- Containment.

The US NRC describes how multiple layers of defence are specific applications of the principle of defence-in-depth to the arrangement of instrumentation and control systems used by a nuclear reactor, providing necessary signals for reactor operation and reactor protection.

These layers comprise the Control system, Reactor Protection system, Engineered Safety Feature system (ESF) and Monitoring and Indication system. The basic defence function is performed by assuring quality and operation according to the limiting conditions for normal operation. The control system maintains steady-state operating conditions, assures an adequate margin to trip settings, and suppresses excursions imposed by operational transients before protective action is required. This requires instrumentation that measures the corresponding nuclear plant process variables. These variables are essentially the same parameters required by the protection system. If adverse conditions occur and the Control systems are not able to control the reactor in an acceptable operating band, the Reactor protection system shuts down the reactor. If accident conditions progress further, ESF systems continue to support the barriers to prevent radiological release: see Figure 3.1.

![Figure 3.1: Example of NPP Defence-in-Depth.](image-url)
3.3 General principles used for designing the safety system

The safety system is designed to ensure the effectiveness of the barriers in case of pre-determined accidents in a nuclear power plant. The safety system design also includes a definition of the protection channels and a calculation of the signal set-point for safety system actuation.

Integrity of the fuel cladding

Typical limits which are applicable during Category I (Normal Operation) and Category II (Faults of Moderate Frequency) and which assure cladding integrity are as follows:

- DNB must not occur, which is ensured by maintaining a DNBR greater than the limiting value to give a 95% probability with 95% confidence that DNB is not occurring at any point in the core. For Westinghouse plants, this limit is 1.3 or 1.17 depending on the analysis method used.
- Fuel centre line temperature ($T_{CL}$) must be maintained at less than the fuel melt temperature, corrected for end of life (EOL) burn-up conditions. For a Westinghouse design $T_{CL}$ must be less than 2590°C which corresponds to a fuel rod linear power of 590 W/cm.
- Cladding stress must be maintained at less than the yield stress.
- Cladding strain is maintained at less than 1.0%.
- Fuel rod internal pressure is maintained at less than 155 bar.

To prevent a DNB condition in the core, the actual heat flux must be less than the critical heat flux by a certain margin everywhere in the core.

The limits applied during Category III (Infrequent Faults) and Category IV (Limiting Faults) which assure integrity of the cladding are:

- Peak cladding temperature (PCT) during a LOCA will not exceed 1200°C.
- By limiting PCT the zirconium-steam reaction is limited and thus cladding oxidation. This reaction increases significantly above 1200°C.
- Cladding oxidation will not exceed 17% of the total cladding thickness to prevent excessive loss of local cladding strength and ductility.
- Hydrogen generation (due to zirconium-water reaction) will not exceed 1% of the hydrogen generated if all the zirconium surrounding the fuel were to react; this is to prevent accumulation of an explosive mixture of hydrogen in the
containment. A hydrogen burn in the containment could exceed its design pressure.

- Coolable core geometry must be maintained to prevent cladding failure from blocking coolant channels.
- Long term cooling must be provided to assure that the decay heat can be removed, preventing additional core damage.

During the LOCA condition the reactor should be tripped. Decay heat is transferred from the fuel to the coolant and dictates the cladding temperature. To limit the PCT, decay heat has to be limited which can be managed by limiting the maximum heat flux during normal operation.

Limiting $F_0$ (defined in Module 1) in the core during normal operation means limiting the maximal heat flux in the core, which dictates the limit of the PCT during a LOCA.

**Integrity of the reactor coolant system**

The integrity of the second barrier Reactor Coolant System is assured by a set of values for pressure in the RCS. For example a Westinghouse PWR has the following values:

- Normal operating pressure is 154.1 bar.
- Design pressure of the Reactor Coolant System is 171.3 bar, the lift setting of the pressurizer safety valves.
- The Pressure Safety Limit is 110% of the design pressure, which represents 188.6 bar.
- The Reactor Protection System generates a reactor trip signal if the pressurizer pressure exceeds the set-point value of 163.8 bar. The trip prevents the pressure Safety Limit from being exceeded.

**Integrity of the Containment**

The safety design basis for the containment is that it must withstand the pressures and temperatures of a DBA without exceeding the design leak rate. The ESFs must ensure that the release of radioactive material due to a DBA does not exceed the specified values. The values specified are those referring to the reactor's »exclusion area« and the »low population zone«.

**3.4 Reactor protection system**

The system must be capable of generating reactor trip signals and engineered safety features actuation signals, to provide the required degree of protection for all normal operating and accident conditions.

A simplified diagram of the Reactor Protection System is shown in Figure 3.4. The heart of each train of protection is the solid state protection cabinet. The nuclear and process instrument systems send trip signals to the logic trains. There are two complete and independent sets of logic circuits in the reactor protection system.
cabinets. When an unsafe condition is sensed, a trip signal is sent to the protection cabinets. If a reactor trip is required, the protection cabinets send a signal to the reactor trip breakers. Tripping of these breakers removes power from the control rod drive mechanisms, allowing the rods to drop into the reactor core. If an ESF actuation is required, the protection cabinets actuate the appropriate safeguard devices. Permissive signals are also provided to the logic trains to allow automatic or manually initiation of interlocks and bypasses.

![Diagram of reactor protection and engineering safety features](image)

**Figure 3.4:** Reactor Protection and Engineering Safety Features System.

To ensure that the system performs its required functions under all credible accident conditions, it is designed with a high degree of reliability, and incorporating the following features:

**Redundancy**
Parameters that indicate an unsafe condition have redundant measurement systems. Sufficient redundant measurements are provided to allow a coincident logic scheme such that a spurious measurement neither causes nor prevents a reactor trip or safeguard feature actuation. Two trains of protection logic are provided. Either train is capable of initiation of the required protective function.

**Independence**
Each channel of measurement and each train of protection is physically and electrically independent. The components of different channels are physically separated, penetrate the containment at different locations and are supplied by independent electrical power supplies. Independence ensures that a single malfunction or casualty will interrupt only one of the redundant channels or trains.
Diversification
Several different methods are used to perform similar functions or to indicate the same casualty. For example, reactor power is detected by nuclear instrumentation measuring the neutrons which leak out of the core, and by the process instrumentation measuring differential temperature across the core, which is proportional to reactor power. Certain reactor trips are automatically or manually bypassed at low power when they are not required for safety. The bypass circuit design is such that the bypass is automatically removed whenever the permissive conditions are not met.

Fail-Safe
The system is designed to supply the safest signal or a failure. Loss of power to a trip bistable will supply a trip signal to the protection logics. Loss of power to the rod control system will result in the rod control clusters falling into the core.

Testability
The reactor protection system is capable of being calibrated or tested at power without the loss of protection.

Control System interactions do not degrade reliability
The variables for the Control system are essentially the same parameters required by the protection system. As a result, the primary sensor and transmitting equipment that is used in the protection system is also used for the control system. The control system is maintained separate and distinct from the protection system by physical separation and electrical isolation, and receives the plant process signals monitored by the protection system through isolation amplifiers. This ensures there is no feedback from the control system to the protection system.

List of reactor trips
The reactor protection system generates a reactor trip when a nuclear and/or process variable reaches its predetermined value (trip set point). The function of a reactor trip system is to shut down the reactor to prevent core Safety Limits from being exceeded. Below is a list of the origins of reactor trip signals:

- Manual trip (operator judgment);
- Nuclear instrumentation trips;
- Pressurizer pressure and level trips;
- RCS flow trips;
- Steam generator level trip;
- Turbine trip;
- Overtemperature (OTΔT) trip;
- Overpower (OPΔT) trip;
- Reactor trip on ESFAS signals.

Overtemperature (OTΔT) trip (example)
The overtemperature $\Delta T$ trip is designed to protect against a departure from nucleate boiling (DNB) which would cause a large decrease in the heat transfer coefficient between the fuel rods and the reactor coolant, resulting in high fuel cladding temperatures.

In the protection system, the indicated loop $\Delta T$ is used as a measure of reactor power and is compared with an $OT\Delta T$ set point that is automatically varied, depending on $T_{avg}$, the pressurizer pressure and the axial flux difference (AFD).

If the $\Delta T$ signal exceeds the calculated set point, the affected channel will be tripped, and if two or more channels are simultaneously tripped, the reactor will be tripped.

The $T_{avg}$ term in the $OT\Delta T$ equation acts to lower the trip set point above normal full power $T_{avg}$. This is necessary because the heat capacity of the reactor coolant water is greater at higher temperatures. The increased average temperature also reduces the margin to DNB.

The pressure term reduces the $OT\Delta T$ set point when the pressure is lower than rated since this condition would reduce the margin to DNB.

The AFD term is a function of $\Delta q$ and reduces the value of the trip set-point to reflect an increase in the hot channel factors. $\Delta q$ is referred to as the axial flux difference and is defined as:

$$\Delta q = P_T - P_B.$$ 

$P_T$ and $P_B$ are the reactor power at the top and the bottom half of the core as a percentage of the rated thermal power (nominal power).

The overtemperature $\Delta T$ trip provides protection against DNB only if:
- The transient encountered is slow with respect to piping transient delays from the core to the temperature detectors and
- The reactor coolant pressure is within the bounds set by the high and low pressure trips.

**Reactor Coolant Low Flow trips (example)**

Low flow trips are provided to protect the core from DNB following a loss of coolant flow accident where there is not enough coolant flow to remove the heat generated by the fuel. This trip is necessary since the $\Delta T$ trips do not respond fast enough to ensure adequate core protection. The four diverse methods for sensing a low flow condition are as follows:
- Measured flow in the reactor coolant piping.
- Detecting an open position of the reactor coolant pump breakers.
- Sensing an undervoltage condition on the reactor coolant pump buses.
- Sensing an underfrequency condition on the reactor coolant pump buses.

Low Flow Trip
Each reactor coolant loop has three flow measuring circuits that generate a low flow trip signal if any two-of-the-three circuits sense a flow below 90% of the normal full flow.

RCP Breaker Opening
The trip signal from the reactor coolant pump breaker is provided to anticipate probable loss of forced flow through the core and the resultant thermal transient.

RCP Undervoltage Trip
This trip is provided for protection following a complete loss of power to the RCPs. A voltage condition below 70% of nominal voltage, as sensed by undervoltage relays, directly trips the reactor to prevent DNB.

RCP Underfrequency Trip
The purpose of this trip is to provide reactor protection following a major network frequency disturbance. If an underfrequency condition below 47.7 Hz exists on the reactor coolant pump buses, all RCP breakers and the reactor are tripped. This is done because an underfrequency condition will slow down the pumps, thereby reducing their coastdown time following a pump trip. The proper coastdown time is required in order for the reactor heat to be removed during the tripping of the control rods. In principle, a rapid decrease in electrical frequency can decelerate the reactor coolant pumps faster than a complete loss of power.

Engineered Safety Features (ESF)
The function of the ESF is to mitigate the consequences of Category 3 and 4 events (DBA); this is performed by designing the appropriate systems to:
- Protect the fuel and fuel cladding;
- RCS integrity;
- Ensure containment integrity;
- Limit fission product releases to the environment.

The ESF concept is considered in the design of the following systems and subsystems:
1. Containment Systems:
   - Containment;
   - Containment Heat Removal System;
   - Fission Product Removal and Control Systems;
   - Containment Isolation System;
   - Containment Combustible Gas Control System.
2. Emergency Core Cooling System (ECCS).
3. Control Room Heating, Ventilation, and Air Conditioning
(HVAC) System.

4. Reactor Building Annulus Negative Pressure Control System.

The design basis for the containment is that it must withstand the pressures and temperatures of a DBA without exceeding the design leak rate. The ESFs must ensure, that the release of radioactive material due to a DBA does not result in doses exceeding the specified limiting values.

The design basis of the Containment Heat Removal System is to reduce the containment temperature and pressure following a LOCA or main steam line break accident, by removing thermal energy from the containment atmosphere.

The Fission Product Removal and Control Systems function to reduce or limit the amount of fission products released following a LOCA or fuel handling accident.

The Containment Isolation System allows the normal or emergency passage of fluids through the containment boundary while minimizing the release of fission products from the containment following a LOCA or fuel handling accident.

The safety design basis of the Containment Combustible Gas Control System is to maintain the hydrogen concentration below 4.0 per cent by volume in the containment.

The ECCS is designed to cool the reactor core and provide shutdown capability following the initiation of a LOCA, RCCA ejection accident, SLB or FLB, or SGTR.

The safety design basis of the Control Room HVAC Systems is to provide radiation protection to personnel occupying the control room during the duration of an accident.

The safety related function of the Reactor Building Annulus Negative Pressure Control System is to achieve a negative pressure differential relative to the outside immediately after a LOCA.

The Reactor Protection System (RPS) automatically initiates the Engineered Safety Features (ESF) through various Engineered Safety Features Actuation Signals (ESFAS). Specific plant conditions will generate more than one ESFAS and some ESFAS’s will generate other ESFAS’s. Examples of some ESFAS signals are as follows:

- Safety Injection Signal (SIS);
- Containment Isolation Signal - phase A (CISA);
- Control Room Ventilation Isolation Signal (CRVIS);
- Main Steam Line Isolation Signal (MSLIS);
- Auxiliary Feedwater Actuation Signal (AFAS);
- Containment Spray Actuation Signal (CSAS);
- Others.
**Safety Injection Signal (SIS)**
A SIS is generated by one of the three adverse conditions or manually as follows:
- Low steam line pressure;
- Low pressurizer pressure;
- HI-1 containment pressure;

The functions of the SIS are to shutdown the reactor, if this has not already occurred, maintain the reactor shutdown, provide cooling to the reactor, and maintain containment integrity. The following actions will occur upon the receipt of an SIS. A reactor trip signal is generated. The diesel generators are started, but the generators will not assume any load. The SI sequencers are actuated. This will start the following loads:
- Safety Injection Pumps;
- Residual Heat Removal (RHR) Pumps;
- Essential Service Water (ESW) Pumps;
- Component Cooling Water (CCW) Pumps;
- Containment Spray Pumps (if a CSAS is present);
- Motor Driven Auxiliary Feedwater Pumps;
- Others.

The proper actuation of the ECCS requires many valves to change or be in a specific position. An SIS is sent to these valves to ensure their correct position.

### 3.5 Questions

1. Into which categories are predetermined accident scenarios grouped?
2. List the main barriers in a pressurized water reactor.
3. What are the layers of defence-in-depth and how are they arranged?
4. What does safety system design include?
5. How is the integrity of the first barrier assured during Category 1 and 2 events?
6. How is the integrity of the first barrier assured during Category 3 and 4 events?
7. How is the integrity of the second barrier assured?
8. What is the safety design basis for the containment?
9. State the design features incorporated by the RPS to ensure a high degree of reliability.
10. What is the function of the reactor trip? List the categories of reactor trip signals.
11. What is the purpose of the overtemperature \( \Delta T \) trip?
12. What do reactor coolant low flow trips provide?
13. What is the function of the Engineered Safety Features?
14. In which systems and subsystems is the ESF concept considered?
15. What is the function of the Safety Injection Signal (SIS)?
Learning objectives

After completing this chapter, the trainee will be able to:
1. Describe general considerations regarding limits and conditions (LCs) for normal operation.
2. List the items for which limits and conditions for normal operation are established.

4.1 General considerations

The basic concepts of operational limits and conditions were discussed in the first part of this module (Chapter 1). The limits and conditions for normal operation are a major subset of the total list of OLCs and they ensure safe operation thus they ensure that the assumptions of the safety analysis report are valid and that the established safety limits are not exceeded in the operation of the plant. In the LCs for normal operation an acceptable margin between allowable normal operating values and the required safety system settings is established to avoid undesirably frequent actuation of safety systems.

The LCs for normal conditions take into account allowable values of the reactor process variables, including reactivity control, reactor protection, core cooling, coolant (and moderator) chemistry, and requirements for containment and accident management systems, electrical systems, and other systems. LCs also address requirements for minimum operable equipment, minimum staffing in the control room and elsewhere, and requirements for operator action in the case abnormal conditions are encountered. Abnormal conditions may include violation of limits on process variables or operability requirements.

Operability requirements for the various modes of normal operation state the number of systems or components important to safety that are either in the operating condition or in standby condition. These operability requirements together define the minimum safe plant configuration for each mode of normal operation. Where operability requirements are not met to the extent intended, the actions to be taken to manoeuvre the plant to a safer state, such as power reduction or reactor shutdown, are specified, and the time allowed to complete the action is also stated.

Requirements for restart of the plant after a normal or forced shutdown are included. Given the higher associated risks during startup of the power plant, the operability requirements for this mode
are more stringent than those permitted for operational flexibility in power operation. All conditions encountered in normal operation, especially shutdown and start-up, must be considered in establishing minimum equipment operability requirements.

Next in this chapter a sample list of items is presented for which limits and conditions for normal operation are generally established. Guidance and recommendations for these limits and conditions for normal operation are provided by IAEA Safety Guide NS-G-2.2 (Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants).

### 4.2 Reactivity control

**Negative reactivity requirements**
The minimum negative reactivity available in reactivity control devices is such that the degree of subcriticality assumed in the safety report is reached immediately after shutdown from any operational state and relevant accident conditions. To maintain the specified degree of subcriticality for an indefinite period of time after shutdown, additional means provided in the design, such as borated water or other poisons, are used for compensation of temperature, xenon or other transient reactivity effects.

The required negative reactivity is specified in terms of the information available to the reactor operator such as control rod positions, liquid poison concentration or neutron multiplication factors.

**Reactivity coefficients**
Where the safety report indicates the need, limits are stated for the reactivity coefficients for different reactor conditions to ensure that the assumptions used in the accident and transient analyses remain valid through out each fuelling cycle.

**Positive reactivity insertion rates**
Positive reactivity insertion rate limits are stated and compliance ensured either by the reactivity system logic or by special limitations to be observed by operating personnel in order to avoid reactivity-related accident conditions leading to excessive fuel temperatures.

**Reactor core neutron flux monitoring**
Instrumentation requirements for adequate neutron flux monitoring at all reactor power levels including start-up and shutdown conditions are stated. These may include the necessity for provision of independent neutron sources in the core in order to assure the minimum detector response during shutdown and start-up operation.

**Reactivity control logic**
Special reactivity control logic, or control rod and/or absorber
patterns, together with control rod reactivity values are stated where it is necessary to ensure that specified limitations regarding permissible neutron flux differences, power peaking factors and power distribution for various modes of normal operation are met. Proper control of neutron flux distribution ensures that the limiting fuel temperatures and heat flux, and the initial conditions assumed in the accident analyses, are not exceeded. Where appropriate, proper calculational methods or measuring techniques are provided to enable the reactor operator to determine compliance.

**Reactivity control devices**
Operability requirements, including redundancy or diversity requirements described in the safety report for reactivity control devices and their position indicators, are stated for the various modes of normal operation. These requirements comply with the requirements for reactivity control logic and meet the negative reactivity requirements presented above.

**Reactivity differences**
Limits on permissible reactivity differences between predicted and actual critical configurations of reactivity control devices are stated, and conformance is verified during initial criticality, after every major refuelling, and at specified intervals. The cause of any significant differences is evaluated and necessary corrective actions are taken.

**Liquid poison systems**
The concentration, storage and temperature limits affecting solubility are stated for all liquid poison systems and appropriate measures specified to ensure the detection and correction of deviations from these limits. Operability requirements to ensure proper actuation and functioning of these systems are also stated.

**Boron dilution prevention**
Requirements for the boron concentration in the coolant are established if necessary to maintain an acceptable shutdown margin. The boron concentration is monitored to assure that it is not reduced below the prescribed level.

**Reactor protection system**
Operability requirements for reactor protection and other safety system instrumentation and logic, together with limits on response times, instrument drift and accuracy, where appropriate, are stated. The interlocks required by the safety report are identified and appropriate operability requirements stated.

### 4.3 Core cooling

**Coolant temperature**
The limits of coolant temperature (maximum or minimum) and the rate of temperature change are stated for the various modes of normal
operation to ensure that the specified safety limits of core parameters are not exceeded, and to ensure that temperatures affecting coolant system integrity are maintained within the appropriate bounds.

**Coolant pressure**
Limits on permissible reactor coolant system pressure are stated for the various modes of normal operation. For some purposes, e.g., in order to take account of limitations in material properties, these operational limits are stated in conjunction with other parameters such as temperature or coolant flow. In such cases, the relations are stated clearly and any curves or calculational techniques required to ensure that permissible conditions are not exceeded are provided.

Likewise, special requirements are stated where applicable. The selection of limits is made so that the initial conditions assumed for the various accident analyses are not exceeded and the integrity of the primary coolant system is maintained.

**Reactor power and power distribution**
Limits to the reactor power and core power distribution are established to ensure that the limits on the fuel linear power density (kW/m) and DNBR are not exceeded.

**Safety and relief valves**
Operability requirements are stated regarding the number of safety and/or relief valves required for the reactor coolant system. For direct cycle boiling water plants, this system includes the steam system relief and safety valves. Pressure settings for valve actuation are stated. Selection of these values is such that reactor system integrity is maintained under all operational states.

**Steam generators**
Operability requirements consistent with those described in the safety report are stated for the steam generators. These requirements include the operability of emergency feedwater systems and of safety and isolation valves of the steam system, as well as satisfactory water quality and specified limitations on water level and on minimum heat exchange capacity.

**Coolant system leakage**
Leakage limits are such that the coolant inventory is maintained by normal make-up systems and system integrity is maintained to the degree assumed in the safety report. In establishing leakage limits, consideration is given to the permissible limits of contamination of the environment of secondary systems by leaking media. Operability requirements are stated regarding the reactor coolant leakage detection or measuring systems.

**Radioactivity in the coolant**
Limits regarding the permissible specific activity of the reactor coolant are stated in order to ensure the protection of personnel and
the environment, as well as to provide a measure of fuel integrity as discussed in the safety report.

**Ultimate heat sink**  
The ultimate heat sink is usually the river, lake or sea from which cooling water for equipment and the condensers is drawn. In some cases dry or wet cooling towers are also used. Limitations on power production levels consistent with the cooling capability of these sinks are specified.

**Decay heat removal**  
Minimum requirements for the availability of the decay heat removal system are established, and actions to be taken in case this essential function is not satisfactory are prescribed.

**Emergency core cooling**  
Operability requirements for the various systems used for emergency core cooling are stated. These include pump and valve operability, adequacy of coolant injection and recirculation flow, integrity of the piping system, and specified limitations on the minimum available volume of fluids in the subsystems which are part of the emergency core cooling.

### 4.4 Coolant and moderator chemistry

**Reactor coolant chemical quality**  
In addition to the pressure and temperature limitations mentioned, limits are stated for coolant chemical quality; for instance, in water-cooled reactors its conductivity, pH value, oxygen content and impurities such as chlorine and fluorine are important.

**Moderator and cover gas system**  
As appropriate, limits regarding moderator temperature, chemical quality and containment levels are stated. Limits regarding permissible concentrations of explosive gas mixtures in the cover gas are also stated. In this regard, operability requirements for on-line process monitoring equipment are specified.

**Failed fuel detection**  
Where on-line measurement of coolant activity is used to monitor the fuel cladding integrity during operation, minimum provisions for the detection and, where appropriate, identification of failed or suspect fuel elements are stated.

### 4.5 Containment systems and accident management systems

Operability requirements for containment systems are stated and
include the conditions for which containment integrity is not required. Permissible leakage rates are specified, and the operability and condition of the following are stated: isolation valves, vacuum breaker valves, actuation devices, filtration, cooling, dousing and spray systems, combustible gas control and analysing systems, venting and purging systems, and associated instrumentation. The operational conditions specified are such that the release of radioactive materials from the containment system is restricted to those leakage paths and rates assumed in the accident analyses. Precautions in controlling access are specified in order to ensure that the containment system’s effectiveness is not impaired.

Where remote shutdown instrumentation and control are provided in the plant design to allow for the possible loss of habitability of the main control room, the operability requirements for the essential items (e.g. temperature, pressure, flow, neutron flux) are stated to permit the plant to be shutdown and maintained in a safe condition from a location or locations outside the main control room.

### 4.6 Electrical power systems

Requirements for the availability of electrical power sources are stated for all operational states. These include off-site sources, on-site generation (diesels, gas turbines, including associated fuel reserves), batteries and associated control, protective, distribution and switching devices. The operability requirements are such that sufficient power is available to supply all safety-related equipment required for the safe shutdown of the plant and for the mitigation and control of accident conditions. The operability requirements determine the necessary power, redundancy of supply lines, maximum permissible time delay, and necessary duration of the emergency power supply.

### 4.7 Other systems

**Ventilation systems**
Where applicable, appropriate limits are established on the operability of the ventilation system where such systems are provided for the purpose of controlling airborne radioactivity within stated limits, or for support of a safety system.

Where secondary containment is provided, it is ventilated and kept under appropriate negative pressure as described in the safety report in order to ensure that any possible direct leakage remains below the value specified. Appropriate limits in terms of pressure or leakage rates are stated.

**Seismic monitors**
Where applicable, operability requirements for seismic monitoring
instrumentation are stated. Settings are established for alarms or for any corrective action consistent with the safety report. The number of devices specified is sufficient to ensure that any required automatic action is initiated at the specified limits.

**Fuel handling**

Operational requirements and procedures are stated for fuel and absorber handling. These measures include limits on the quantity of fuel which can be handled simultaneously and, if required, on the temperature of cooling water and decay heat of irradiated fuel. Consideration is given to the prevention of movements of heavy equipment, such as a fuel-shipping cask, above stored irradiated fuel. If appropriate, the operability of fuel handling equipment is stated.

Provision is made for monitoring the core reactivity during fuel loading or refuelling operations to ensure that the reactivity requirements are met. The procedures and instrumentation required for such monitoring are specified.

To ensure that operations which might give rise to nuclear excursions or radiation hazards are not undertaken during fuel movements, requirements for communication between the fuel handling personnel and the operating personnel in the control room are stated.

**Irradiated fuel storage**

Conditions for irradiated fuel storage are stated and include the minimum cooling capability of the spent fuel cooling system and minimum water level above the fuel, the prohibition of storage of fuel in any position other than that designated for irradiated fuel, the minimum storage reserve capacity, and the appropriate reactivity margins to guard against criticality in the storage area. Appropriate radiation monitoring is also specified for the irradiated fuel storage area.

**New fuel storage**

The criteria for new fuel storage are stated. Any special measures to avoid criticality of new fuel during handling or storage are also stated. When required, fuel enrichment is also verified before insertion into the core.

**Core verification**

After any core alteration, the location of fuel and other in-core components is confirmed in accordance with a written procedure, to ensure that every item is located in its correct place.

**Radiation monitoring**

Operability requirements for radiation monitoring instrumentation, including effluent monitoring, are stated. These requirements must ensure that appropriate areas and release paths are adequately monitored in accordance with the requirements of radiological protection and of the regulatory body, and that an alarm or appropriate
action is initiated when the prescribed radiation or activity limit is exceeded.

**External events**
In the case of an external event requirements are stated for the assessment and inspection of nuclear power plant systems for possible damage (before resumption of power operation). These external events include:
- Man-induced events such as an airplane crash, pressure waves, and toxic and corrosive gases, and
- Extreme natural events such as tornados, earthquakes and floods.

### 4.8 Questions

1. What do the limits and conditions for normal operation ensure?
2. What may abnormal conditions include?
3. What are the operability requirements for the various modes of normal operation?
4. What actions are taken when the operability requirements are not met?
5 OPERATIONAL LIMITS AND CONDITIONS
DOCUMENT – TECHNICAL SPECIFICATIONS

Learning objectives
After completing this chapter, the trainee will be able to:
1. Explain the purpose of the Technical Specifications.
2. Describe the structure of the Technical Specifications.

5.1 Introduction

The main threat to the public from a nuclear power plant is the uncontrolled release of radioactive material into the environment. Four physical barriers are designed in a nuclear power plant to prevent the release of radioactive material:
- The fuel;
- The fuel cladding;
- The reactor coolant system (RCS);
- The containment.

The design criteria of a nuclear power plant include an analysis of the plant response to transients and accidents that can occur at different frequencies and have different implications.

The primary purpose of the accident analysis is to confirm the integrity of the barriers and that the risk to the public and the personnel of nuclear power plants is within the limits that are specified in the regulations. In the accident analysis some initial assumptions (criteria) are chosen which are in general always conservative. These assumptions in the analysis deal with:
- Design features of the nuclear power plant (number of loops, type of containment, number of fuel elements in the core etc.);
- Operability of the systems and components;
- Operating characteristics of devices;
- Values of process variables (flow, temperature, pressure, power distributions peaking factors, etc.);
- Maintenance of equipment and buildings.

Every nuclear power plant must operate according to the initial assumptions used for accident analysis and this is the purpose of the Technical specifications (TS). The operators must maintain the state of the plant and plant parameters within the limits given in the Technical specifications.

Operating according to the TS means assuring the validity of the selected input assumptions for accident analysis and thereby ensuring the validity of the analysis. The TS form a part of the operating
In the past, the original specifications, the so-called "customized Technical Specifications", were custom-made for each plant and covered the main aspects of radiological operation. They did not have a standard meaning or form and were different from plant to plant. Due to the rapid increase in the number of nuclear power plants in the world and growing disagreements between individual plants the U.S. NRC (Nuclear Regulatory Commission) in 1972 decided what should and what should not be included in the TS. The Commission initiated a programme that would manufacture generic "standard technical specifications" with a standard content and format. This would thus generate a basis upon which power plants could set up their own Technical specifications.

5.2 An example of TS (Westinghouse PWR)

The Technical specifications consist of five sections:
1. Definitions;
2. Safety Limits (SL) and Limiting Safety System Settings (LSSS);
3. Limiting Conditions for Operation (LCO) and Surveillance Requirements (SR);
4. Design features;
5. Administrative control.

Definitions
This section defines important terms that appear in the TS. The terms, each with their own definition, appear in capital letters everywhere in the TS. This section also defines the Operational Modes, which form the basis for all operational requirements in the TS, and standard abbreviations (for frequency intervals). These Operational modes are: Power operation, Startup, Hot standby, Hot shutdown, Cold shutdown, and Refuelling. They are defined by the values of $k_{eff}$, $T_{avg}$ and by the percentage of rated thermal power. The standard abbreviations refer to the length of the time interval; for example "D" stands for "DAY" (24 hours), "M" for "MONTH" (31 days), etc. They are used in the Surveillance requirements, where it is stated how frequently often each type of surveillance should be implemented.

Examples of the definition of a term:
 a) OPERABLE – OPERABILITY
A system, subsystem, train, component or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified function(s), and when all necessary attendant instrumentation, controls, electrical power, cooling or seal water, lubrication or other auxiliary equipment required for the system, subsystem, train, component, or device to perform its
function(s) are also capable of performing their related support function(s).

b) PRESSURE BOUNDARY LEAKAGE
PRESSURE BOUNDARY LEAKAGE shall be leakage (except steam generator tube leakage) through a nonisolable fault in a Reactor Coolant System component body, pipe wall, or vessel wall.

**Safety Limits and Limiting Safety System Settings**
Safety Limits are restrictions on certain measured variables to ensure the integrity of the barriers against the release of radioactive material into the environment.

**First Safety Limit**
The first safety limit refers to the DNBR and to the linear power density of fuel rods in the core. It puts restrictions on the combination of three measured variables, namely the average coolant temperature (its maximum value), the thermal power and the pressure in the primary circuit. The first safety limit ensures the integrity of the cladding.

**Second Safety Limit**
The second safety limit relates to the pressure in the primary circuit. It ensures the integrity of the pressure boundary of the RCS.

**Limiting Safety System Settings**
One of the important functions of the reactor protection system is to shut down the reactor to prevent its operation in conditions where the safety limits could be exceeded and by doing so to assure the integrity of the fuel cladding and the RCS.

In this section all reactor trip signals and their settings which trigger an automatic reactor shutdown are collected. When analysing the settings it is assumed that the plant previously operated in accordance with the TS.

**Limiting Conditions for Operation (LCO)**
This forms the most extensive part of the TS. In this section Limiting conditions of operation (LCO) are defined such as: the minimum acceptable operational capability of a system (subsystem, equipment ...), the maximum or minimum allowable values of process variables, parameters, constants, etc. If the LCO are not met, the necessary action must follow. Instructions are written in the Action statement. The Action statement specifies the time during period which the system (device, parameter, etc.) must be returned to the state required by the corresponding LCO. If the LCO cannot be corrected in time, the Action statement gives further instructions on the time frame and the Operational mode the plant should be brought into.

Each LCO has a corresponding Surveillance requirement (SR). The
SR dictates how often the system (subsystem, equipment, parameter, etc.) needs to be tested, calibrated or otherwise controlled to check that it follows the LCO requirement. If surveillance is performed correctly and in a timely manner, we can assume that the LCO requirements are also met during the time periods between individual tests.

Each LCO requirement refers to a specified Operational mode. The APPLICABILITY statement defines which Operational mode a certain LCO refers to.

LCOs for operation have the following subsections:
- Applicability;
- Reactivity control system;
- Power distribution limits;
- Instrumentation;
- Reactor cooling system;
- Emergency core cooling systems;
- Containment systems;
- Plant systems;
- Electrical power systems;
- Refuelling operations;
- Special test exceptions;
- Radioactive effluents.

**Applicability**
This should not be confused with the »applicability« that is a part of the LCO requirement. Basic rules on how to use the whole section of Limiting conditions for operation are set out in the Applicability subsection.

Below the limiting condition for operation for reactivity control is shown.

**Example:**

**LIMITING CONDITIONS FOR OPERATION**

**LCO**

The SHUTDOWN MARGIN shall be greater than or equal to 1.6 % delta k/k.

**APPLICABILITY:** MODES 1 and 2.

**ACTION:**

With the SHUTDOWN MARGIN less than 1.6 % delta k/k, immediately initiate and continue boration at greater than or equal to 15 m$^3$/h of a solution containing greater than or equal to 7000 ppm boron or equivalent until the required SHUTDOWN MARGIN is restored.
Module XI: Operational Limits and Conditions

Design features
Important design features of the plant that are not addressed in other sections are listed in this section. Their amendment would affect the safety of the plant and invalidate the conclusions of the safety analysis. The following are examples:
- Basic design characteristics of the containment, core and reactor cooling system;
- Capacity and limitations for the spent fuel pit;
- Component cycle limits;
- Others.

Administrative controls
This Section lists the administrative requirements for safe operation of the plant and the measures used in cases of violation of safety margins and operating conditions. Considered are the responsibilities of leading management personnel, the composition and qualifications required for the shift operators, and the minimum requirements for procedures and programmes required for reporting, archiving and reviews.

Basis
Basis are provided at the end of the technical specifications. Each Basis explains the reasons for the specifications given in the sections "Safety limits and limiting safety system settings" and "Limiting conditions for operation and surveillance requirement". Each Basis explicitly connects restrictions in the specification to the safety analysis. It should be noted that the Basis are not part of the technical specifications.

5.3 Questions

1. What is the primary purpose of the accident analysis?
2. With what do the initial assumptions in the analysis deal?
3. What does operating according to the Technical Specifications assure?
4. Which sections are included in the Technical Specifications?
5. What terms does the section Definitions deal with?
6. What is collected in the section Limiting Safety System Settings?
7. What follows if a Limiting Condition for operation is not met?
8. What does an action statement specify?
9. What is the purpose of Surveillance requirements?
10. What does an applicability statement assert?
11. Describe the subsections of the limiting conditions for operation.
12. What does the section Administrative controls list?
13. What is the purpose of the Basis? What do they explicitly connect? Are the Basis statements part of the Technical Specifications?
6 CASE STUDY

Learning objectives
After completing this chapter, the trainee will be able to:
1. Describe the interrelationship between a safety limit, a safety system setting and an operational limit.

The interrelationship between a safety limit, a safety system setting and an operational limit is explained in Figure 6.1. For clarity, the example illustrates only the case in which the critical parameter of concern is the fuel cladding temperature.

It is assumed for the purposes of Figure 6.1 that a correlation has been established in the safety analysis report between a monitored parameter (in this case the coolant temperature) and the maximum fuel cladding temperature, for which a safety limit has been established. The safety analysis shows that actuation of the safety system by the monitored coolant temperature at the safety system setting prevents the fuel cladding temperature from reaching the safety limit set, beyond which releases of significant amounts of radioactive material from the fuel might occur.

Range of steady state operation
The monitored parameter is kept within the steady state range by the control system or by the operator in accordance with the operating procedures.

Alarm setting exceeded (curve No. 1)
The monitored parameter can exceed the steady state range as a result of load changes or imbalance of the control system. For example, if the temperature rise reaches an alarm setting, then the operator will be alerted and takes action to supplement any automatic systems in reducing the temperature to the steady state values without allowing the temperature to reach the operational limit for normal operation. The delay in the operator’s response is taken into consideration.

Operational limit exceeded (curve No. 2)
Limits for normal operation are set at any level between the range of steady state operation and the actuation setting for the safety system, on the basis of the results of the safety analysis. Normally there are margins between the alarm settings and the operational limits in order to take account of routine fluctuations arising in normal operation. There is also a margin between the operational limit and the safety system setting to allow the operator to take action to control a transient without activating the safety system. If the operational limit is reached and the operator takes corrective action to prevent the safety system setting being reached, then the transient will be of the form of curve 2.
In the event of a malfunction of the control system, or an operator error, or for other reasons, the monitored parameter reaches the safety system setting at point A with the consequence that the safety system is actuated. This corrective action only becomes effective at point B owing to inherent delays in the instrumentation and equipment of the safety system. The response is sufficient to prevent the safety limit being reached, although local fuel damage cannot be excluded.
Safety limit exceeded (curve No. 4)

In the event of a failure that exceeds the most severe one that the plant was designed to cope with, or a failure or multiple failures in a safety system, it is possible for the temperature of the cladding to exceed the value of the safety limit, and hence significant amounts of radioactive material are released. Additional safety systems are actuated by other parameters to bring other engineered safety features into operation to mitigate the consequences, and measures for accident management are activated.

6.1 Questions

1. Why can a monitored parameter exceed the steady state range?
2. What will happen when the monitored parameter (coolant temperature) reaches the alarm setting?
3. What is the purpose of the margin between the operational limit and the safety system setting?
4. What will happen when the monitored parameter reaches the safety system setting?
5. When it is possible for the temperature of the cladding to exceed the value of the safety limit? What are the consequences and which systems are actuated to mitigate them?
7 REFERENCES


The views expressed in this document do not necessarily reflect the views of the European Commission.